



PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 7, 2018

MuckRock News
Emma Best
Dept. MR 56717
411A Highland Ave.
Somerville, MA 02144-2516

Dear Emma Best:

This is a final response to your Freedom of Information Act (FOIA) request dated June 25, 2018 that we received on June 25, 2018.

You asked for copies of all drafted, submitted or received SF-716 forms (<https://www.archives.gov/files/isoo/security-forms/sf716.pdf>) produced from January 1, 2001 through December 31, 2017.

I am enclosing a copy of the requested records for 2013 through 2017 consisting of 20 pages.

The business unit has conducted a search for the records responsive to your request for 2001 through 2012. There are no documents specifically responsive to this portion of your request.

You may contact me, the FOIA Public Liaison, Dalyce Harrop, to discuss your request at:

Internal Revenue Service
Disclosure Office 12
1973 N Rulon White Blvd MS 7000
Ogden, UT 84404
(801) 620-6098

The FOIA Public Liaison responds to FOIA and Privacy Act requests for copies of documents maintained by the IRS. There is no provision in either Act to resolve tax, collection, or processing issues and our staff is not trained to answer questions regarding those issues. If you need assistance with tax related issues, you may call the IRS toll free number at 1-800-829-1040.

If you are unable to resolve your FOIA dispute through the FOIA Public Liaison, the Office of Government Information Services (OGIS), the Federal FOIA Ombudsman's Office, offers mediation services to help resolve disputes between FOIA requesters and Federal agencies. The contact information for OGIS is:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road--OGIS
College Park, MD 20740-6001
202-741-5770
877-684-6448
ogis@nara.gov
ogis.archives.gov

You have the right to file an administrative appeal within 90 days of the date of this letter. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and reconsider your request and the agency's decision. I've enclosed Notice 393, *Information on an IRS Determination to Withhold Records Exempt From the Freedom of Information Act - 5 U.S.C. 552*, to explain your appeal rights.

If you have any questions please call Tax Law Specialist Jody M Mecham ID #1000141871, at 801-620-7635 or write to: Internal Revenue Service, Disclosure Scanning Operation – Stop 211, PO Box 621506, Atlanta, GA 30362. Please refer to case number F18176-0076.

Sincerely,



Dalyce Z Harrop
Acting Disclosure Manager
Disclosure Office 12

Enclosures
Responsive records
Notice 393

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Internal Revenue Service	Fiscal Year: 2013
--	--------------------------

Point of Contact: (Name and phone number) Lois Stith, 202-317-3558
--

Reporting Categories

Please use actual dollar figures.

1. Personnel Security <i>(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)</i>	\$2,050,068.00
2. Physical Security <i>(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)</i>	
3. Classification Management <i>(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)</i>	
4. Declassification <i>(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)</i>	
5. Protection and Maintenance for Classified Information Systems <i>(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)</i>	\$30,000.00
6. Operations Security and Technical Surveillance Countermeasures <i>(include personnel and operating expenses associated with OPSEC and TSCM)</i>	
7. Professional Education, Training, and Awareness <i>(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)</i>	\$20.00
8. Security Management, Oversight, and Planning <i>(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))</i>	
9. Unique Items <i>(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)</i>	
TOTAL <i>(sum of items 1-9)</i>	\$2,080,088.00

Narrative: Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.

1. Cost of initiating and adjudicating clearance investigations - includes cost of reinvestigations of NBU employees in moderate risk positions.
5. Cost of ISDN to maintain STE connection.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified Information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. Personnel Security: A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

National Agency Check: Include only when used for basis for granting a clearance.

Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

Polygraph: Substantive examinations in security screening process.

2. Physical Security: That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. Classification Management: The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. Declassification: The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. Protection and Maintenance for Classified Information Systems: A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. Professional Education, Training, and Awareness: The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. Security Management, Oversight, and Planning: Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. Unique Items: Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. Name of Department/Agency : Self-explanatory.

2. Reporting Categories: List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. Totals: The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. Narrative: In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Internal Revenue Service

Fiscal Year: 2014

Point of Contact:

(Name and phone number) Bernetta Bizzell, 240-240-5518

Reporting Categories

Please use actual dollar figures.

1. Personnel Security

(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

\$1,213,444.00

2. Physical Security

(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

3. Classification Management

(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

4. Declassification

(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

5. Protection and Maintenance for Classified Information Systems

(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

\$22,000.00

6. Operations Security and Technical Surveillance Countermeasures

(include personnel and operating expenses associated with OPSEC and TSCM)

7. Professional Education, Training, and Awareness

(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

8. Security Management, Oversight, and Planning

(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

\$50,000.00

9. Unique Items

(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

TOTAL

(sum of items 1-9)

\$1,285,444.00

Narrative: Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.

1. The difference in the costs from FY 2013 (\$2,050,088) to FY 2014 (\$1,213,444) was \$836,444, and can be attributed directly to the reduction in the number of NSC investigation initiated in FY 2014. In FY 2013 the total number NSC investigation initiated was 596, and in FY 2014 the number initiated dropped to 208.

3) Cost for STE line for about 30 sites

8) % of (1) Security Specialist salary for security related duties

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified Information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. Personnel Security: A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

National Agency Check: Include only when used for basis for granting a clearance.

Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

Polygraph: Substantive examinations in security screening process.

2. Physical Security: That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. Classification Management: The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. Declassification: The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. Protection and Maintenance for Classified Information Systems: A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. Professional Education, Training, and Awareness: The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. Security Management, Oversight, and Planning: Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. Unique Items: Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should not include costs associated with the broader area of assets protection.

1. Name of Department/Agency : Self-explanatory.

2. Reporting Categories: List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. Totals: The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. Narrative: In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Internal Revenue Service

Fiscal Year: 2015

Point of Contact:
(Name and phone number) Bernetta Bizzell (240) 613-5518

Reporting Categories

Please use actual dollar figures.

1. Personnel Security

(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

\$1,610,015.00

2. Physical Security

(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

\$5,921.00

3. Classification Management

(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

\$15,000.00

4. Declassification

(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

5. Protection and Maintenance for Classified Information Systems

(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

6. Operations Security and Technical Surveillance Countermeasures

(include personnel and operating expenses associated with OPSEC and TSCM)

\$3,222.00

7. Professional Education, Training, and Awareness

(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

\$65,000.00

8. Security Management, Oversight, and Planning

(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

9. Unique Items

(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

TOTAL

(sum of items 1-9)

\$1,699,158.00

Narrative: Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.

- Item 1. Increased OPM investigative costs. This category represents 96% of the total annual cost increase.
- Item 2. Installation of alarms and locks.
- Item 3. Installation of STE (telephone line and travel).
- Item 8. Portion of annual salary (1/2) for one (1) 0080 position in management responsibilities.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified Information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. Personnel Security: A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

National Agency Check: Include only when used for basis for granting a clearance.

Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

Polygraph: Substantive examinations in security screening process.

2. Physical Security: That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. Classification Management: The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. Declassification: The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. Protection and Maintenance for Classified Information Systems: A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. Professional Education, Training, and Awareness: The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. Security Management, Oversight, and Planning: Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. Unique Items: Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. Name of Department/Agency: Self-explanatory.

2. Reporting Categories: List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. Totals: The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. Narrative: In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Internal Revenue Service (Personnel Security)

Fiscal Year: 2016

Point of Contact:

(Name and phone number) Gordon Rice (202-317-6388)

Reporting Categories

Please use actual dollar figures.

1. Personnel Security

(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

\$2,026,537.00

2. Physical Security

(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

3. Classification Management

(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

4. Declassification

(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

5. Protection and Maintenance for Classified Information Systems

(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

6. Operations Security and Technical Surveillance Countermeasures

(include personnel and operating expenses associated with OPSEC and TSCM)

7. Professional Education, Training, and Awareness

(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

8. Security Management, Oversight, and Planning

(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

9. Unique Items

(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

TOTAL

(sum of items 1-9)

\$2,026,537.00

Narrative: Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.

Personnel Security - the \$416,522 increase from last year report is a result from an increase in the number of requests and increased cost of investigations. This total accounts for 82% of the increase from last year. Additional staffing costs account for the remaining 18% difference.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified Information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. Personnel Security: A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

National Agency Check: Include only when used for basis for granting a clearance.

Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

Polygraph: Substantive examinations in security screening process.

2. Physical Security: That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. Classification Management: The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. Declassification: The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. Protection and Maintenance for Classified Information Systems: A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. Professional Education, Training, and Awareness: The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. Security Management, Oversight, and Planning: Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. Unique Items: Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. Name of Department/Agency : Self-explanatory.

2. Reporting Categories: List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. Totals: The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. Narrative: In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Internal Revenue Service

Fiscal Year: 2017

Point of Contact:
(Name and phone number) David Abercrombie 240-613-6618

Reporting Categories

Please use actual dollar figures.

1. Personnel Security <i>(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;">\$1,678,993.00</div>
2. Physical Security <i>(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;"></div>
3. Classification Management <i>(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;">\$50,000.00</div>
4. Declassification <i>(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;"></div>
5. Protection and Maintenance for Classified Information Systems <i>(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;"></div>
6. Operations Security and Technical Surveillance Countermeasures <i>(include personnel and operating expenses associated with OPSEC and TSCM)</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;"></div>
7. Professional Education, Training, and Awareness <i>(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;"></div>
8. Security Management, Oversight, and Planning <i>(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;">\$50,000.00</div>
9. Unique Items <i>(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;"></div>
TOTAL <i>(sum of items 1-9)</i>	<div style="border: 1px solid black; padding: 2px; width: 150px;">\$1,778,993.00</div>

Narrative: Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.

1. decrease is due to the reduction in the number of re-investigations that were due in FY 2017, both in investigation costs and salary to work these cases.
3. increase due to program development of process and procedures for the receipt of classified material from other agencies and maintenance of TSDN lines
8. increase due to establishment of secure rooms for TSDN connection and increased management requests related to classified information

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified Information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. Personnel Security: A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

National Agency Check: Include only when used for basis for granting a clearance.

Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

Polygraph: Substantive examinations in security screening process.

2. Physical Security: That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. Classification Management: The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. Declassification: The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. Protection and Maintenance for Classified Information Systems: A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. Professional Education, Training, and Awareness: The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. Security Management, Oversight, and Planning: Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. Unique Items: Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. Name of Department/Agency : Self-explanatory.

2. Reporting Categories: List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. Totals: The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. Narrative: In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.



Department of the Treasury
Internal Revenue Service

Notice 393

(Rev. September 2016)

Information on an IRS Determination to Withhold Records Exempt From The Freedom of Information Act – 5 U.S.C. 552

Appeal Rights

You may file an appeal with the Internal Revenue Service (IRS) within 90 days after we (1) deny you access to a record in whole or in part; (2) have made an adverse determination as to your category as a requester; (3) deny your request for a fee waiver or reduction; or (4) have advised you that no records responsive to your request exist. You may file an appeal within 10 days when a request for expedited processing has been denied.

Your appeal must be in writing, must be signed by you, and must contain:

Your name and address,

- Description of the requested records,
- Date of the request (and a copy, if possible),
- Identity of the office and contact on the response letter, and
- Date of the letter denying the request (and a copy, if possible)

Mail your appeal to:

IRS Appeals

Attention: FOIA Appeals
M/Stop 55202
5045 E. Butler Ave.
Fresno, California 93727-5136

Judicial Review

If we deny your appeal, or do not address an issue raised in your appeal within 20 days (excluding Saturdays, Sundays, or legal public holidays) after the date we receive your appeal, you may file a complaint in United States District Court in the district in which (1) you reside; (2) your principal place of business is located; (3) the records are located; or (4) the District of Columbia. A complaint may be filed within 10 days (excluding Saturdays, Sundays, or legal public holidays) after the date we receive your appeal if your appeal is from an adverse determination of a request for expedited processing. If you choose to file suit before receipt of a final determination by the Appeals office, the administrative appeals process may cease.

The rule for effecting service of judicial process upon the Internal Revenue Service is set forth in Federal Rule of

Civil Procedure 4(i). In addition to service upon the United States, as set forth in Rule 4(i)(1), service must be made upon the Internal Revenue Service by registered or certified mail as set forth in Rule 4(i)(2)(A).

The address of the Internal Revenue Service is: Internal Revenue Service, Attention CC:PA, 1111 Constitution Avenue, N.W., Washington, D.C. 20224.

Exemptions

The Freedom of Information Act, 5 U.S.C. 552, does not apply to matters that are:

(b)(1) • specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified under such executive order,

(b)(2) • related solely to the internal personnel rules and practices of an agency,

(b)(3) • specifically exempted from disclosure by statute (other than section 552b of this title), provided that the statute:

(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or

(B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.

Note: Internal Revenue Code sections 6103 and 6105 are statutes which qualify for exemption 3 treatment. Section 6103 protects the confidentiality of tax returns and information pertaining to a taxpayer collected by the IRS. Section 6105 protects information obtained from a foreign country under a tax treaty.

(b)(4) • trade secrets and commercial or financial information obtained from a person and privileged or confidential,

(b)(5) • inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency,

(b)(6) • personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy,

(b)(7) • records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information:

(A) could reasonably be expected to interfere with enforcement proceedings,

(B) would deprive a person of a right to a fair trial or an impartial adjudication,

(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,

(D) could reasonably be expected to disclose the identity of a confidential source, including a State, local or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or

(F) could reasonably be expected to endanger the life or physical safety of any individual.

(b)(8) • contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions, or

(b)(9) • geological and geophysical information and data, including maps, concerning wells.